AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) A device-to-device authentication system for authenticating ~~whether or not~~ when devices on a network are connected within a certain range, ~~characterized in that~~ comprising:

a first device comprising:

~~each of said devices interconnected via said network has~~ a first mediating device interface for physically ~~accessing~~ connecting a removable mediating device ~~such that said mediating device is removable~~,

a second device comprising:

a second mediating device interface for physically connecting the removable mediating device, and

local environment management means for authenticating that ~~another~~ the first device ~~physically accessing said same mediating device within a predetermined period of time is located in a local environment where contents are available; wherein use of said contents is allowed between said devices in said local environment~~ has physically connected to the removable mediating device within a predetermined period of time before or after the removable mediating device physically connected to the second device,

wherein the first device can use content when the first device is authenticated.

2. (Currently Amended) The device-to-device authentication system according to claim 1, ~~characterized in that~~ wherein:

~~one of said devices~~ the second device is a home server ~~for legitimately acquiring said contents~~,

~~whereas the other device~~ the first device is a client for making a request for ~~said contents~~ the content to ~~said~~ the home server~~ for use~~; ~~wherein~~ and,

in response to ~~confirmation of presence of both said devices on said same home network by said local environment management means, said~~ authentication of the client, the home server provides ~~said contents~~ the content and/or issues a license for ~~said~~ the content ~~contents~~ to ~~said~~ the client.

3. (Currently Amended) The device-to-device authentication system according to claim 1, ~~characterized in that~~ wherein:

two or more home servers are able to be installed on ~~said home~~ the network; and

~~wherein each said~~ at least one of the home ~~server~~ servers provides ~~said contents~~ the content and/or issues a license for ~~said contents to said client~~ the content to a client that is ~~confirmed to be present on said same home network~~ authenticated.

4. (Currently Amended) The device-to-device authentication system according to claim 3, c~~haracterized in that: said~~ wherein the client is able to be ~~received~~ receive provision of ~~said contents~~ the content and/or issuance of ~~said~~ the license from ~~two or more said~~ at least one of the two or more home servers on ~~said same home~~ the network.

5. (Currently Amended) The device-to-device authentication system according to claim 3, ~~characterized in that: said client is able to use said contents acquired from a plurality of home servers on said same home network, and,~~ wherein upon connection to a home server on ~~an other home~~ a second network, ~~said~~ the client is not able to use ~~said contents acquired from said home servers on said home networks other than said other home network~~ the content from the two or more home servers.

6. (Currently Amended) The device-to-device authentication system according to claim 1, ~~characterized in that: said~~ wherein the removable mediating device is capable of retaining predetermined identification information for determining that the first and the second device have connected to the removable mediating device within the predetermined period of time~~; and said local environment management means authenticates that each of said devices is in said local environment based on a fact that each of said devices physically accessing said mediating device reads the same identification information from said mediating device and/or that time at which each of said devices reads the identification information is within a predetermined period of time~~.

7. (Currently Amended) The device-to-device authentication system according to claim 1, ~~characterized in that~~ wherein:

~~said~~ the removable mediating device ~~has~~ comprises a memory for retaining confidential information, for determining that the first and the second device have connected to the removable mediating device within the predetermined period of time, in a secure manner~~;~~

~~one of said devices physically accessing said mediating device is capable of generating said confidential information; and said local environment management means authenticates that each of said devices is located in said local environment based on a fact that said confidential information generated from said one of said devices is able to be acquired by another device via said mediating device within a predetermined period of time~~.

8. (Currently Amended) The device-to-device authentication system according to claim 7, ~~characterized in that: said device generated said~~ wherein the confidential information is erased ~~erases said confidential information~~ after ~~elapse of a~~ the predetermined period of time elapses~~; and said local environment management means authenticates that a device, which is capable of sharing said confidential information prior to loss of said confidential information in said device generated said confidential information, is located in said local environment~~.

9. (Currently Amended) A device-to-device authentication method for authenticating ~~whether or not~~ when devices on a network are connected within a certain range, ~~characterized in that~~ comprising:

~~each of said devices interconnected via said network has a mediating device interface for physically accessing a mediating device such that said mediating device is~~

~~removable; and said device-to-device authentication method, characterized by comprising:~~

physically connecting a removable mediating device to a first physical mediating device interface of a first device;

physically connecting the removable mediating device to a second physical mediating device interface of a second device;

~~a local environment management step of~~ authenticating ~~that another~~ that the first device physically ~~accessing said same~~ connected to the mediating device within a predetermined period of time ~~is located in a local environment where contents are available; and a content using step of allowing use of said contents between said devices in said local environment~~ before or after the removable mediating device physically connected to the second device; and

allowing the first device to use content when the first device is authenticated.

10. (Currently Amended) The device-to-device authentication method according to claim 9, ~~characterized in that~~ wherein:

~~one of said devices~~ the second device is a home server ~~for legitimately acquiring said contents~~,

~~whereas the other device~~ the first device is a client for making a request for ~~said contents~~ the content to ~~said~~ the home server ~~for use~~; ~~wherein, in said content using step~~ and, in response to ~~confirmation of presence of both said devices on said same home network, said~~ authentication of the client, the home server provides ~~said contents~~ the content and/or issues a license for ~~said~~ the content ~~contents~~ to ~~said~~ the client.

11. (Currently Amended) The device-to-device authentication method according to claim 9, ~~characterized in that~~ wherein:

two or more home servers are able to be installed on ~~said home~~ the network; and

~~wherein, in said content-using step, each said~~ at least one of the home ~~server~~ servers provides ~~said contents~~ the content and/or issues a license for ~~said contents to said client~~ the content to a client that is ~~confirmed to be present on said same home network~~ authenticated.

12. (Currently Amended) The device-to-device authentication method according to claim 11, ~~characterized in that: in said content-using step, said~~ wherein the client is able to be ~~received~~ receive provision of ~~said contents~~ the content and/or issuance of ~~said~~ the license from ~~two or more said~~ at least one of the two or more home servers on ~~said same home~~ the network.

13. (Currently Amended) The device-to-device authentication method according to claim 11, ~~characterized in that: in said content-using step, said client is able to use said contents acquired from a plurality of home servers on said same home network, and,~~ wherein upon connection to a home server on ~~an other home~~ a second network, ~~said~~ the client is not able to use ~~said contents acquired from said home servers on said~~

~~home networks other than said other home network~~ content from the two or more home servers.

14. (Currently Amended) The device-to-device authentication method according to claim 9, ~~characterized in that: said mediating device is capable of retaining~~ further comprising:

storing predetermined identification information, for determining that the first and the second device have connected to the removable mediating device within the predetermined period of time, in the removable mediating device ~~; and in said local environment management step, each of said devices is authenticated in said local environment based on a fact that each of said devices physically accessing said mediating device reads the same identification information from said mediating device and/or that time at which each of said devices reads the identification information is within a predetermined period of time~~.

15. (Currently Amended) The device-to-device authentication method according to claim 9, ~~characterized in that: said mediating device has a memory for retaining~~ further comprising:

storing confidential information, for determining that the first and the second device have connected to the removable mediating device within the predetermined period of time, in a secure manner in the removable mediating device~~; one of said devices physically accessing said mediating device is capable of generating said confidential information; and in said local environment management step, each of said~~

~~devices is authenticated in said local environment based on a fact that said confidential information generated from said one of said device is able to be acquired by another device via said mediating device within a predetermined period of time~~.

16. (Currently Amended) The device-to-device authentication method according to claim 15, ~~characterized in that: said device generated said~~ wherein the confidential information is erased ~~erases said confidential information~~ after ~~elapse of a~~ the predetermined period of time elapses~~; and in said local environment management step, a device, which is capable of sharing said confidential information prior to loss of said confidential information in said device generated said confidential information, is authenticated that located in said local environment~~.

17. (Currently Amended) A communication apparatus for using content ~~contents~~ on a network within a predetermined allowable range, ~~characterized by~~ comprising:

a mediating device interface for physically ~~accessing~~ connecting a removable mediating device ~~such that said mediating device is removable~~; and

local environment management means for authenticating that the apparatus and a device have physically connected to the ~~that another device physically accessing said same~~ mediating device within a predetermined period of time between connections, to control the use of the content ~~is located in a local environment where contents are available; and content-using means for using said contents legitimately in said local environment~~.

18. (Currently Amended) The communication apparatus according to claim 17, ~~characterized in that~~ further comprising:

means for providing the content and/or issuing a license for the content when the device and the apparatus are authenticated,

wherein ~~said~~ the communication apparatus operates as a home server for providing ~~said contents on said~~ content on the network;~~ and~~

~~said content using means provides said contents and/or issues a license for said contents only to a device confirmed to be present on said same home network by said local environment management means~~.

19. (Currently Amended) The communication apparatus according to claim 17, ~~characterized in that~~ further comprising:

mean for receiving provision of the content and/or a license for the content when the device and the apparatus are authenticated,

wherein ~~said~~ the communication apparatus operates as a client for making a request for ~~said contents~~ the content to a home server ~~for use on said~~ on the network~~;~~ ~~said content using means receives provision of said contents and/or issuance of a license for said contents only from a home server confirmed to be present on said same local environment by said local environment management means~~.

20. (Currently Amended) The communication apparatus according to claim 19, ~~characterized in that: two or more home servers are able to be installed under said local environment; said content using~~ wherein the means ~~receives~~ for receiving receives

provision of ~~said~~ the content ~~contents~~ and/or issuance of a license for ~~said~~ the contents from ~~said~~ the two or more home servers ~~confirmed to be present on said same local environment~~ authenticated by ~~said~~ the local environment management means.

21. (Currently Amended) The communication apparatus according to claim 19, ~~characterized in that: said content-using means is able to use said contents acquired from a plurality of home servers under said same local environment, and,~~ wherein upon connection to a second home server on ~~an other home~~ a second network, ~~said~~ the client is not able to use ~~said~~ the content ~~contents~~ acquired from ~~said home servers under said local environment other than said other home network~~ the home server on the network.

22. (Currently Amended) The communication apparatus according to claim 17, ~~characterized in that: said~~ wherein the removable mediating device is capable of retaining predetermined identification information for determining that the communication apparatus and another device have connected to the removable mediating device within the predetermined period of time~~; said mediating device interface reads said identification information in response to physical access from said mediating device; and said local environment management means authenticates that another device, which reads the same identification information from said mediating device and/or reads the identification information within a predetermined period of time, is in said local environment of said local environment management means~~.

23. (Currently Amended) The communication apparatus according to claim 17, ~~characterized in that: said~~ wherein;

the removable mediating device comprises a memory for retaining confidential information, for determining that the communication apparatus and another device have connected to the removable mediating device within the predetermined period of time, in a secure manner~~; said communication apparatus further has a confidential information generation apparatus for generating said confidential information; said mediating device interface writes said confidential information to said memory of said mediating device in response to physical access from said mediating device; and said local environment management means authenticates that another devices is located in said local environment of said local environment management means based on a fact that said confidential information generated from said local environment management means is able to be acquired by said another device via said mediating device within a predetermined period of time~~.

24. (Currently Amended) The communication apparatus according to claim 23, ~~characterized in that: said mediating device has a memory for retaining confidential information in a secure manner; said mediating device interface takes out said confidential information from said memory of said mediating device in response to physical access from said mediating device; and~~ wherein, ~~said~~ the local environment management means authenticates that ~~a~~ the another device, which reads same confidential information from ~~said~~ the mediating device and/or reads ~~said~~ the

confidential information within a predetermined period of time, is located in ~~said~~ the local environment of ~~said~~ the local environment management means.

25. (Currently Amended) The communication apparatus according to claim 23, ~~characterized in that: said~~ wherein the confidential information is ~~lost after elapse of~~ erased after a predetermined period of time from generation elapses~~; and said local environment management means authenticates that a device, which is capable of sharing said confidential information prior to loss of said confidential information, is located in said local environment~~.

26. (Currently Amended) A ~~computer~~ computer-readable medium storing a program ~~described in a computer-readable format so as to execute a process, on a computer system,~~ for causing a computer to execute a method for authenticating whether or not devices on a network are connected within a certain scope, ~~characterized in that~~ the method comprising:

~~each of said devices interconnected via said network has a mediating device interface for physically accessing a mediating device such that said mediating device is removable; and said computer program, characterized by comprising: a local environment management step of authenticating that another device physically accessing said same mediating device within a predetermined period of time is located in a local environment where contents are available; and a content using step of allowing use of said contents between said devices in said local environment~~

authenticating that a first device physically connected to a removable mediating device within a predetermined period of time before or after the removable mediating device physically connected to a second device,

allowing the first device to use content when the first device is authenticated.